Check Point
SOFTWARE TECHNOLOGIES LTD.

19 July 2017

R80.10

Release Notes

Check Point
INFINITY

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Check Point R80.10

For more about this release, see the R80.10 home page
http://supportcontent.checkpoint.com/solutions?id=sk111841

Latest Version of this Document

Download the latest version of this document
http://supportcontent.checkpoint.com/documentation_download?ID=54802

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R80.10 Release Notes.

Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package
http://downloads.checkpoint.com/dc/download.htm?ID=54846.
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

Revision History

Date	Description
19 July 2017	Added support for UTM-1 Edge N in Backward Compatibility Gateways (on page 14)
02 July 2017	Added Hyper-V support in Supported Platforms (on page 14). Added Smart-1 405 and 410 support in Check Point Appliances (on page 12).
01 June 2017	Updated requirements for Security Management Server / Standalone in Open Server Hardware Requirements (on page 13).
16 May 2017	First release of this document

Contents

Introduction

Thank you for installing Check Point R80.10 - The cyber security platform of the future. This release integrates R80 management features with new Security Gateway features and enhancements.

Important Links

For more about R80.10 and to download the software, see the R80.10 Home Page: sk111841
http://supportcontent.checkpoint.com/solutions?id=sk111841

- Before you upgrade, see the latest upgrade tools on the Home Page.
- Read the Known Limitations: sk110519
  http://supportcontent.checkpoint.com/solutions?id=sk110519
- See issues resolved in this release: sk110518
  http://supportcontent.checkpoint.com/solutions?id=sk110518

Visit the Check Point Checkmates Community https://community.checkpoint.com/

- Start discussions
- Get answers from experts
- Join the API community to get code samples and share yours

Visit http://www.checkpoint.com/architecture/infinity/ to learn more about Infinity R80.10.

What's New

R80.10 creates a breakthrough in Check Point Security Gateway, matching the R80 security management innovations.

R80.10 is part of **Check Point Infinity**, a consolidated cyber security architecture that spans networks, cloud, and mobile. It provides the highest level of threat prevention against both known and unknown targeted attacks to keep you protected now and in the future.

Security Policy New Architecture

- **Policy Layers and Sub-Policies -** Enable flexible control over the security policy behavior.
  - Build a rule base with layers, each with a set of the security rules. Layers are inspected in the order in which they are defined, giving control over the rule base flow and precedence of security functionality. If an "Accept" action is done in a layer, inspection continues in the next layer.
  - Sub-Policies (Inline Layers) are sets of rules that you attach to specific rules. If the rule is matched, inspection continues in the sub-policy attached to the rule. If the rule is not matched, the sub-policy is skipped.
    For example, a sub policy can manage a network segment or branch office.
  - Policy Layers and Sub-Policies can be managed by specific administrators, according to their permission profile, allowing easy responsibility delegation in the team.

- **Unified Security Policies**:
  - Access Control policy unifies the Firewall, Application Control & URL Filtering, Content Awareness, and Mobile Access Software Blade policies.
  - Threat Prevention policy unifies the IPS, Anti-Virus, Anti-Bot, Threat Extraction, and Threat Emulation Software Blade policies.

Access Control Policy

- New Content Awareness Software Blade adds visibility and control over data transfers in the network traffic, using data types based on content, file types, and direction.
- Application Control enhancements:
  - Added Recommended Services to Applications for easier configuration of the unified policy.
  - Applications matched on Recommended Services, customized set of services, or Any service.
  - New Protocol Signature added to Service object, to enhance policy matching security and granularity.
- Mobile Access policy rules can be defined in the main, unified Access Control Policy:
  - Unified rules can define access from different client types to the same resources.
  - Explicit rules can block specified Mobile Access traffic.
  - Ability to define access to resources from specified client types only.
- Security Zones: Group interfaces of gateways into Security Zones for new Source and Destination definitions.
- Fully Qualified Domain Names (FQDN): Additional mode for Domain objects, to match fully qualified domain names with forward DNS lookup.
- Acceleration of Domain Objects, Dynamic Objects, and Time Objects.
- New tracking options in Unified Rule Base.
- Improvement of policy installation time duration.

Threat Prevention Policy

- Multiple profiles for each Security Gateway, to enforce granular Threat Prevention policies.
- Faster Threat Prevention policy installation.
- IPS is integrated into the Threat Prevention policy Rule Base and policy installation.
- Threat Prevention profiles support IPS protection activation based on property tags.

Significant Improvements and New Features

- The new **Check Point Labs** lets you experience new features and send feedback to Check Point. The first Check Point Labs feature lets you see information on Session changes before you publish.
- **VPN and Mobile Access Enhancements**
  - VPN multicore performance with CoreXL multicore scalability for VPN traffic inspected by Next Generation Firewall, Next Generation Threat Prevention, and Next Generation Threat Extraction Software Blades.
  - NAT-T support for Site-to-Site VPN.

  - TLS 1.2 support for Mobile Access and portals.
  - Multiple login options with multi-factor authentication schemes for users of different clients and portals. See Multiple Login Option Support (on page 20).
  - A Mobile Access transparent Reverse Proxy, allowing external users to access internal resources, without the Mobile Access portal.
- **Identity Awareness Enhancements**
  - Up to 200,000 Identity sessions per gateway.
  - Gateway REST API to manage identities from 3rd party or customized system.
  - Identity Collector - New agent that collects identity information from different sources (AD and ISE), for large environment scalability.
  - New RADIUS Accounting attribute parsing and IPv6 support.
  - Enhanced handling of nested user groups for AD LDAP using LDAPv3.
  - Enforce remote access client type in access role.
  - Detect users located behind HTTP proxy using X-Forward-For header granularity per Access Control Policy Layer.
- **Threat Prevention Enhancements**
  - Threat Emulation MTA (Mail Transfer Agent) support in VSX. You can run MTA for each VS instance.
  - Threat Extraction support for VSX Gateways.
  - Snort rules can be imported from SmartConsole.
  - Importing Custom Indicators (IoC) is supported from SmartConsole
- **NAT Enhancements**
  - Improved scalability of hide NAT on high end multicore gateways, allowing maximum usage of available hide ports by dynamically assigning available ports to the cores. See sk103656 http://supportcontent.checkpoint.com/solutions?id=sk103656.
  - IP Pool NAT performance enhancement - CoreXL multicore scalability for IP Pool NAT connections.
- **Gaia Enhancements**
  - Netflow support for IPFIX (with NAT and IPv6 flow records).
  - IPv6 DHCP relay with ClusterXL (Security Gateway and VSX modes).
- **Dynamic Routing Enhancements**
  - RIPng with VRRPv2.
  - SNMP enhancements for routing.
  - BGP 4-Byte AS and Local AS.
- **VSX Enhancements**
  - 64-bit support for VSX Gateways, increasing concurrent connections capacity.
  - Content Awareness for VSX Gateways.
- **ClusterXL Enhancements**
  - The MAC Magic value is acquired automatically and is backward compatible with gateways that were configured manually in earlier versions.
  - For VSX Clusters in load sharing environments (VSLS), Backup members can communicate with external networks and receive updates, in addition to Active and Standby members.
  - Connectivity Upgrades now support synchronization of Dynamic Routing.

Management Enhancements

These enhancements were first introduced in R80.

- **Multi-Domain Security Management**
  - Unified architecture and management console for Security Management and Multi Domain Security Management.
  - New and improved views for Domain management and Global Assignment.
- **Role-based & Concurrent Administration** - Several administrators can work in parallel on the same security policy, with granular and flexible privilege delegation to each administrator.
  - A new advanced locking mechanism ensures administrators do not overwrite each others' work.
  - Rich administrator profiles for exact privileges each administrator will have, including managing specific policies or network segments, viewing specific logs, and conducting security operations, such as installing policy.
- **Secured Automation and Orchestration** - CLI and API for security management enables full integration with 3rd party systems and automation of daily operations. Automation and SmartConsole management operations are allowed based on the same privilege profile.
- **Faster Day to Day Operations**
  - Integrated logging to see all logs related to a rule in the same screen.
  - Detailed rule information of who created the rule and when, hit counts, and user-defined data, such as ticket numbers.
  - Enhanced search capabilities to quickly find any rule or object in the system.
  - Enhanced Management High Availability synchronizes only changes between servers, significantly improving efficiency.
- **Next Generation Logs, Events and Reports**
  - Analyze hundreds of millions of logs per day with graphical views and reports, customized to address specific requirements.
  - Logging, monitoring, and report aspects also available in the Web-based interface.
  - Free-text search of logs and events with auto-suggest and favorites, with results in seconds.
- **New and Enhanced Revision Management Capabilities**
  - Built-in automatic policy revision.
  - Install a specific version of policies.
  - Change to a specific version of IPS package.
- **Cloud Demo -** Experience R80.10 management scenarios on any computer. sk103431 http://supportcontent.checkpoint.com/solutions?id=sk103431
- **vSEC Controller -** Natively integrates with the leading private and public cloud platforms: VMware vCenter & NSX, CISCO ACI, Amazon Web Services (AWS), Microsoft Azure, and OpenStack.
  vSEC Controller provides dynamic security policy and visibility, which automatically adapts to changes in the cloud environments. This provides simple automated security across physical, virtual, and cloud environments, from a single unified management solution.

Behavior Changes

- **Management**
  - Management API commands and the SmartView Web-based interface replace the **Management Portal**. Use the API commands to install a policy and show a list of Gateways and Servers. Use SmartView to see logs.
  - The new tags for objects replace the renaming of object **colors**. You can name a tag according to a color. The tags make it easier to manage objects in SmartConsole.
  - New and improved management abilities replace the Database Revision function. To learn about the enhanced Revisions Management in R80 and higher, see sk113615 http://supportcontent.checkpoint.com/solutions?id=sk113615.
  - The `mdsstop` and `mdsstart` commands on the Multi-Domain Server are the only way to **start and stop Domain Management Servers** function. Most Domain Management Server components are handled in one process. This reduces memory consumption and CPU usage.
- **Logs, Events, and Reports**
  - The Logs tab of the SmartConsole Logs & Monitor view replaces **SmartLog** and **SmartView Tracker**. The Logs tab allows you to search through logs with simple and fast searches. Search results are fast and immediately show the log records.
  - SmartEvent replaces SmartReporter and SmartEvent Intro.
  - Scheduled reports have been integrated to SmartConsole, and are no longer available from SmartEvent legacy GUI.
- **Threat Prevention and IPS**
  - The new IPS Optimized Profile replaces the Recommended Profile with excellent security and improved gateway performance. When upgrading with the Recommended Profile, we recommend that you change to the Optimized Profile.
  - Additional granularity in Threat Prevention permission profiles - Set permissions for IPS Updates.
  - User Center authentication is synchronized with Management Servers to allow IPS and Threat Prevention updates without explicit login to the User Center. This applies only to users with permissions to run updates.
  - New IPS Protections are marked as "Staging" by default. The Staging configuration can be changed from the **Threat Prevention profile** > **IPS**. You can search and filter Staging protections from the **Protections** view, and see corresponding logs. This replaces the follow up flag.
- **Software Blades**
  - **Session Authentication** and **UserAuthority** are replaced by Identity Awareness.
  - Overviews, which were part of the Threat Prevention and Application Control tabs in R77 versions, are now shown in the **Logging and Monitoring** view. This requires SmartEvent activation and license.
  - VPN Traditional Mode is replaced by VPN Simplified Mode.

Licensing

Contact Account Services mailto:accountservices@checkpoint.com?subject=Licensing Issues for all license issues.

Supported Upgrade Paths

CPUSE is the installation and upgrade method supported for this release. To learn more about CPUSE, see sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

Upgrade with the **Supported Methods** for your current installation.

From R80 to R80.10:

Component	Supported Methods
Security Management Server	CPUSE Upgrade CPUSE Clean Install
Multi-Domain Server	

From R75.40, R75.45, R75.46, R75.47, R75.40VS, R76, R77, R77.10, R77.20, R77.30 to R80.10:

Component	Supported Methods
Security Management Server	CPUSE Upgrade CPUSE Clean Install Advanced Database Migration
Multi-Domain Server	
Security Gateway	CPUSE Upgrade CPUSE Clean Install
VSX	CPUSE Upgrade (from R77 only) Earlier versions: Use instructions in sk101518 http://supportcontent.checkpoint.com/solutions?id=sk101518

To upgrade from R77.20 or R77.30 with the Add-on: It is not necessary to uninstall the Add-on. Remove these unsupported features: Modbus support with the Application Control Software Blade, "SAML" Cloud Connector for web based single sign on.

Note: User Defined reports will be migrated during the upgrade to the SmartConsole reports. Report Scheduling and email server definitions will not be migrated and need to be defined.

Required Disk Space

Before installation or upgrade, CPUSE verifies that enough free disk space is available. If the space available is not sufficient, a message shows what is required.

This table shows the disk space required for some packages.

<table>
<tr><th>Installation or Upgrade Type</th><th>Management Server or Standalone</th><th>Security Gateway</th></tr>
<tr><td>R80.10 Clean Install</td><td colspan="2" rowspan="2">The minimum required unpartitioned disk space is the highest value of one of these:
Size of the current root partition.
The used space in the current root partition plus 3 GB.
If the used space is more than 90% of the root partition, then 110% of the size of the current root partition.</td></tr>
<tr><td>R80.10 Major Upgrade (from pre-R80)</td></tr>
<tr><td>R80.10 Minor Upgrade from R80</td><td>3.3GB in root partition and 2.2GB in log partition</td><td>Not relevant</td></tr>
</table>

If you do not have enough disk space, you can use the Logical Volume Manager (lvm) to increase the disk space of logical volumes on Gaia. This space is taken from the unallocated disk space, which is usually used for snapshots and upgrades. See sk95566 http://supportcontent.checkpoint.com/solutions?id=sk95566.

Required Disk Space for Multi-Domain Security Management:

Before you run a clean install of R80.10 on Multi-Domain Servers, make sure that at least **10 GB** of free disk space in the root partition is available. For an environment with many Domain Management Servers, more than 10 GB of free disk space is often required.

Check Point Appliances

Standalone and Management Servers boot by default with 64-bit on clean install and upgrade to R80.10.

Note - If you revert an R80.10 upgrade, the appliance will still boot with 64-bit, even if it was originally 32-bit.

Management Servers

Component	Smart-1 25b, 205, 210, 225, 405, 410	Smart-1 50, 150, 3050, 3150
Security Management	✓	✓
Log Server	✓	✓
SmartEvent Server	✓	✓
Multi-Domain Security Management		✓
Multi-Domain Log Server		✓

Smart-1 25b, 205, and 210 appliances can run Security Management *OR* Log Server *OR* SmartEvent.

Security Gateway and Standalone (Gateway + Management)

The model numbers in this table are for the series of appliances that support R80.10.

Appliance Series	Security Gateway	Standalone (Gateway + Management)
2200	✓	
3000	✓	✓
4000	✓	*
5000	✓	✓
12000	✓	12600*
13000	✓	✓
15000	✓	✓
21000	✓	✓
23000	✓	✓

***** The 4200 appliance does not support a Standalone deployment.
These appliance models do not support a Standalone deployment with their default RAM (4GB): 4400, 4600, 4800, 12200, and 12400. Upgrade these models to at least 8 GB RAM to support a Standalone deployment.

Hardware Health Monitoring

R80.10 supports these Hardware Health Monitoring features for Gaia Check Point appliances:

- **RAID Health:** Use SNMP to monitor the health of the disks in the RAID array, and be notified of volume and disk states.
- **Hardware Sensors:** Use the WebUI or SNMP to monitor fan speed, motherboard voltages, power supply health, and temperatures. Some open servers are supported with an IPMI interface card that requires an IPMI card.

Check Point Appliances	Smart-1
SNMP Hardware sensor monitoring (polling and traps)	✓
WebUI hardware sensor monitoring	✓
RAID monitoring with SNMP	✓

Open Servers:

Hardware Sensors: Use the WebUI or SNMP to monitor fan speed, motherboard voltages, power supply health, and temperatures. Some open servers are supported with an IPMI interface card that requires an IPMI card.

Note - IPMI is an open standard. We cannot guarantee the Hardware Health Monitoring performance on all systems and configurations.

Open Server Hardware Requirements

R80.10 servers are designed to efficiently utilize available hardware resources to maximize performance and scalability. We recommend that you leverage this advantage and use the most powerful hardware available to get the best performance.

Component	Security Gateway	VSX Gateway	Security Management Server / Standalone	Multi-Domain Server
Processor	Intel Pentium IV, 2 GHz or equivalent	Intel Pentium IV, 2 GHz or equivalent	Intel Pentium IV, 2.6 GHz or equivalent	Dual Socket 2x Xeon E5-2609v2 4 cores, 2.5 GHz or equivalent
Total Cores	2	2	2	8
Memory	4 GB RAM	4 GB RAM	6 GB RAM	32 GB RAM
Free Disk Space	15 GB	12 GB + 1 GB per VS	500 GB (Installation includes OS)	1 TB (Installation includes OS)

Supported Platforms

Component	Red Hat Enterprise Linux*	VMware ESXi	Microsoft Hyper-V
Security Management	5.5, 6.8, 7.3	5.x, 6.x	Windows 2012 R2
Multi-Domain Security Management	5.5, 6.8, 7.3	5.x, 6.x	Windows 2012 R2
Security Gateway	Not supported	5.x, 6.x	Not certified**

***** To install R80.10 on Linux, contact Check Point Support.

** For the most updated information about Microsoft Hyper-V, see the *Virtual Machines* section of the Hardware Compatibility List https://www.checkpoint.com/support-services/hcl/.

Maximum Number of Interfaces Supported by Platform

The maximum number of interfaces supported (physical and virtual) is shown by platform in this table.

Platform	Max Interfaces	Notes
Gaia	1024	
Virtual System	256	Includes VLANs and Warp Interfaces
VSX Gateway	4096	Includes VLANs and Warp Interfaces

Backward Compatibility Gateways

R80.10 Management Servers can manage gateways of these versions:

Gateway Type	Release Version
Security Gateway	R75.20, R75.30, R75.40, R75.45, R75.40VS, R75.46, R75.47, R76 R77, R77.10, R77.20, R77.30
VSX	R75.40 VS and higher

R80.10 Management Servers can manage appliance Security Gateways of these versions:

Appliance	Release Version
Security Gateway 80	R75.20.x
UTM-1 Edge N	8.1 and higher
1100 Appliance	R75.20.x, R77.20.x
1200R Appliance	R77.20.x

Appliance	Release Version
1400 Appliance	R77.20.x
60000/40000 Security Platforms	R76SP, R76SP.10, R76SP.20, R76SP.30, R76SP.40 for 61000/41000 R76SP.50 for 61000/41000 and 64000/44000

Logging Requirements

Logs can be stored on:

- A Security Management Server that collects logs from the Security Gateways. This is the default.
- A Log Server on a dedicated machine. This is recommended for organizations that generate many logs.

A dedicated Log Server has greater capacity and performance than a Security Management Server with an activated logging service. On dedicated Log Servers, the Log Server must be the same version as the Management Server.

SmartEvent Requirements

You can install a SmartEvent Server on a Security Management Server or on a different, dedicated server. SmartEvent R80.10 can connect to a different version of Log Server - R77.xx or earlier.

Usually SmartEvent and a Correlation Unit are installed on the same server. You can also install them on separate servers, for example, to balance the load in large logging environments. The Correlation unit must be the same version as SmartEvent.

To deploy SmartEvent and to generate reports, a valid license or contract is required.

Management Console

Console Hardware Requirements

This table shows the minimum hardware requirements for console applications:

Component	Windows
CPU	Intel Pentium Processor E2140 or 2 GHz equivalent processor
Memory	4 GB
Available Disk Space	2 GB
Video Adapter	Minimum resolution: 1024 x 768

Consoles by Windows Platform

SmartConsole is supported on:

- Windows 10 (all editions), Windows 8.1 (Pro), and Windows 7 (SP1, Ultimate, Professional, and Enterprise).
- Windows Server 2016, 2012, 2008 (SP2), and 2008 R2 (SP1).

Gaia WebUI

The Gaia WebUI, also known as the Gaia Portal, is supported on these browsers:

Browser	Supported Versions
Google Chrome	14 and higher
Microsoft Internet Explorer	8 and higher (If you use Internet Explorer 8, file uploads through the Gaia Portal are limited to 2 GB.)
Microsoft Edge	any
Mozilla Firefox	6 and higher
Safari	5 and higher

Build Numbers

Software Blade / Product	Build Number	Verifying Build Number
Gaia	421	`show version all`
Security Gateway	423	`fw ver`
Security Management	187	`fwm ver`
Multi-Domain Server	223	`fwm mds ver`
SmartConsole	991310572	Menu > About Check Point *SmartConsole*

Threat Emulation

The Threat Emulation requirements are different based on the emulation location:

- ThreatCloud - Gaia operating system (64 or 32-bit)
- Local or Remote emulation - Threat Emulation Private Cloud Appliance on the Gaia operating system (64-bit only)

Emulation on local Threat Emulation appliances running R80.10 is not supported.

Mobile Access Requirements

OS Compatibility

Endpoint OS Compatibility	Windows	Linux	Mac	iOS	Android
Mobile Access Portal	✓	✓	✓	✓	✓
Clientless access to web applications (Link Translation)	✓	✓	✓	✓	✓
Endpoint Security on Demand	✓	✓	✓		
SecureWorkspace	✓				
SSL Network Extender - Network Mode	✓	✓	✓		
SSL Network Extender - Application Mode	✓				
Downloaded from Mobile Access applications	✓	✓	✓		
Clientless Citrix	✓	✓	✓		
File Shares - Web-based file viewer (HTML)	✓	✓	✓	✓	✓
Web mail	✓	✓	✓	✓	✓

Browser Compatibility

Endpoint Browser Compatibility	Internet Explorer	Google Chrome	Mozilla Firefox	Macintosh Safari	Opera for Windows
Mobile Access Portal	✓	✓	✓	✓	✓
Clientless access to web applications (Link Translation)	✓	✓	✓	✓	✓
Endpoint Security on Demand	✓	*✓	✓	✓	
SecureWorkspace	✓	*✓	✓		
SSL Network Extender - Network Mode	✓	*✓	✓	✓	
SSL Network Extender - Application Mode	✓	*✓	✓		
Downloaded from Mobile Access applications	✓	✓	✓	✓	
Clientless Citrix	✓		✓		
File Shares - Web- based file viewer (HTML)	✓	✓	✓	✓	Limited support
Web mail	✓	✓	✓	✓	✓

***** Google Chrome support for Mobile Access Portal on-demand clients, such as SSL Network Extender, Secure Workspace, and Endpoint Security on Demand, requires Java JRE 32 bit installed on the end-user's computer.

Identity Awareness Requirements

Identity Agents

See Clients by Windows Platform (on page 20) and Clients by Mac Platform (on page 21) for:

- Identity Agent (Light and Full)
- Identity Agent for Terminal Servers

AD Query

Active Directory for AD Query is supported on:
Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, and 2016.

Endpoint Security Requirements

These are the minimum requirements to enable Endpoint Policy Management on a Security Management Server:

Component	Requirement on all Supported Operating Systems
Number of Cores	4
Memory	8GB RAM
Disk Space	100GB

- Endpoint Security Management Servers are supported on management-only computers or appliances. Standalone (Security Gateway + Management) deployment is not supported.
- Endpoint Security Management Servers are not supported on RedHat Enterprise Linux releases.
- R80.10 Endpoint Security Management Servers can manage E80.62 and E80.64 Endpoint Security Clients for Windows, and E80.64 Endpoint Security Client for Mac.
- These Endpoint Security blades are NOT supported with R80.10 Management:
  URL Filtering, Capsule Docs, and SandBlast Agent blades (Anti-Bot, Forensics, and Threat Extraction and Threat Emulation).

For more information, see the Endpoint Security Client for Windows User Guide for your version and the R80.10 Endpoint Security Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=54801.

Maximum Gateway Cluster Members

Cluster Type	Maximum Number of Supported Cluster Members
ClusterXL	5
Virtual System Load Sharing	13
Third-party	8

Check Point Client Support

Multiple Login Option Support

This release adds multiple login options per gateway with multi-factor authentication schemes, for users of different clients and the Mobile Access portal. For example, configure an option to authenticate with Personal Certificate and Password, or Password and DynamicID for SMS or email.

These features are supported when connected with to an R80.10 gateway that has IPsec VPN or Mobile Access enabled.

Supported Client or Portal	Lowest Supported Version
Mobile Access Portal	R80.10
Capsule Workspace for iOS	1002.2
Capsule Workspace for Android	7.1
Remote Access Clients - Standalone clients	E80.65
Remote Access VPN Blade of the Endpoint Security Suite	E80.65

See the *Mobile Access Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53103 or the *VPN Remote Access Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53105 for details.

Clients by Windows Platform

Microsoft Windows

In this table, Windows 7 support is true for Ultimate, Professional, and Enterprise editions. Windows 8 support is true for Pro and Enterprise editions. All the marked consoles and clients support 32-bit and 64-bit.

Check Point Product	Windows 7 (+SP1)	Windows 8.1	Windows 10
Remote Access Clients E80.x	✓	✓ (with 8.1 Update 1)	✓ (E80.62 and higher)
Capsule VPN Plug-in		✓	✓
SSL Network Extender	✓	✓	✓
UserCheck Client	✓	✓	✓
Identity Agent (Light and Full)	✓	✓	✓
Identity Agent for Terminal Servers	✓		

Microsoft Windows Server

Check Point Product	Server 2008 (SP1-2) 32 / 64	Server 2008R2 (+SP1)	Server 2012	Server 2012 R2 64-bit	Server 2016
UserCheck Client	✓	✓		✓	✓
Identity Agent for Terminal Servers	✓	✓	✓	✓	✓

Note - Identity Agent for Terminal Servers is also supported on XenApp 6.

Clients by Mac Platform

All support is for 64-bit.

Check Point Product	OS X 10.9	OS X 10.10	OS X 10.11	macOS 10.12
Identity Agent	✓	✓	✓	✓
SSL Network Extender	✓	✓	✓	✓
Endpoint Security VPN E80.x or higher	✓ (E80.50.03 and higher)	✓ (E80.60 and higher)	✓ (E80.62 and higher)	✓ (E80.64 and higher)

DLP Exchange Agent

The R80.10 DLP Exchange Agent is supported on:

Windows Server	Exchange Server
2012 R2 64-bit	2010, 2013
2016 64-bit	2016

For earlier server versions, use the R77.30 DLP Exchange Agent.